



PRUEBA DE HABILIDADES PRACTICAS CCNA

EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

ESNEIDER ALEXANDER URREGO HURTADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

PROGRAMA DE INGENIERIA EN TELECOMUNICACIONES

CEAD FACATATIVA

2019



EVALUACIÓN – PRUEBA DE HABILIDADES PRACTICAS CCNA

ESNEIDER ALEXANDER URREGO HURTADO

GRUPO 203092_2

DIPLOMADO DE PROFUNDIZACIÓN CISCO

TUTOR

GIOVANNI ALBERTO BRACHO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

PROGRAMA DE INGENIERIA EN TELECOMUNICACIONES

CEAD FACATATIVA

2019



PRUEBA DE HABILIDADES PRACTICAS CCNA

Resumen

Por medio de este trabajo se pretende dar solución a problemas de telecomunicaciones, problemas que se pueden presentar en el ejercicio de nuestra labor profesional, por medio del desarrollo de estos escenarios y en los requerimientos que este trabajo implica, se adquieren habilidades prácticas y de funcionabilidad, que ayudan a tener conocimiento del funcionamiento de las redes de información.

Por medio de las herramientas que ofrece la universidad con la plataforma Cisco y con el programa Packet Tracer, se da solución a las problemáticas propuestas, usando protocolos, configuraciones, enrutamiento, vectores de distancia, tiempo y estado de enlace.

ABSTRACT

Through this work it is intended to solve telecommunication problems, problems that may arise in the exercise of our professional work, through the development of these scenarios and in the requirements that this work implies, practical and functional skills are acquired , which help to have knowledge of the operation of information networks.

Through the tools offered by the university with the Cisco platform and with the Packet Tracer program, the proposed problems are solved, using protocols, configurations, routing, distance vectors, time and link status.



INDICE

INTRODUCCION	6
Objetivos.....	7
1 ESCENARIO 1- TOPOLOGÍA	8
1.1 DESARROLLO.	8
1.2 PARTE 1 DIRECCIONAMIENTO IP	8
1.3 ASIGNACION DE PARÁMETROS BÁSICOS	8
1.3.1 ASIGNACION DE DIRECCIONES.....	8
1.3.1.1 IP.....	8
1.3.1.2 WS1	9
1.3.1.3 SERVIDOR	9
1.3.1.4 PC1.....	10
1.3.1.5 PC2.....	10
1.3.1.6 PC3.....	11
1.3.1.6 PC4.....	11
1.3 CONFIGURACION BASICA	12
1.4 DIAGNOSTICO DE VECINOS COMANDO CDP.....	12
1.5 PRUEBA DE CONECTIVIDAD CON PING	13
1.6 CONFIGURACION DE DISPOSITIVOS DDE ENRETAMIENTO	15
1.7 ASIGNACION DE PROTOCOLO EIGRP.....	17
1.8 PROTOCOLO DE ENRUTAMIENTO	17
1.9 CONECTIVIDAD DE REDES ENTRE SI	19
1.10 CONFIGURACION DE LISTAS DE CONTROL DE ACCESO	21
1.11 COMPROBACION DE LA RED INSTALADA	23



PRUEBA DE HABILIDADES PRACTICAS CCNA

2 ESCENARIO 2	25
2.1 DESARROLLO	25
2.2 TOPOLOGIA	25
2.3 CIFRADO DE CONTRASEÑAS	25
2.4 CONFIGURACION BASICA	26
2.5 ESTABLECER SERVIDOR TFTP.....	28
2.6 ASIGNAR DHCP	29
2.7 WEB SERVER CON NAT ESTATICO	30
2.8 SERVICIODHCP EN EL SERVIDOR TUNJA.....	31
2.9 LISTAS DE CONTROL DE ACCESO	33
2.10 HOST EN 10,20, Y 30 VLAN ENTRE LOS DESTINOS	35
2.11 PRUEBA DE CONECTIVIDAD.....	38
CONCLUSIONES	39
BIBLIOGRAFIA	40

Tabla delmágenes

Imagen 2 – internet PC-	7
Imagen 3 – web server.....	7
Imagen 4 – _PC- A.....	8
Imagen 5 – PC C.....	8
Imagen 6 – tabla de configuracion basica.....	9
Imagen 7 - configuracion de dispositivo de enrutamiento R1.....	9
Imagen 8 - configuracion de dispositivo de enrutamiento R2.....	10
Imagen 9 - configuracion de dispositivo de enrutamiento R3.....	11
Imagen 10 – balanceo de carga R1	12
Imagen 11 - balanceo de carga R2	12
Imagen 12 - balanceo de carga R3	13
Imagen 13 – Protocolo de enrutamiento.....	14
Imagen 14 - topografia.....	15
Imagen 15 – ping de R1 al Servidor.....	16
Imagen 16 – comprobacion de la red	16
Imagen 17 – conexión de internet en una ethernet	17
Imagen 18 – Conexión basica de los routers	18
Imagen 19 – conexión basica del servidor TFTP	18
Imagen 20 – CONFIGURACION IP.....	19
Imagen 21 – Configuracion Web Server	20
Imagen 22 –IOS linea de interface	21
Imagen 23 – Lista de control acceso	22
Imagen 24 –host VLAN 30 de Bucaramanga acceden a VLAN 10	23
Imagen 25TABLA habilitar VLAN EN CADA SWICH	24
Imagen 26 – enrutamiento OSPF CON AUTENTICACION EN CADA ROUTER	26
Imagen 27 – CONFIGURACION INTERFACES	28
Imagen 28 – configuracion interfaz FO/0 CONEXIÓN R2y R3 EN OSPF	31
Imagen 29 –SERVICIO DHCP EN EL ROUTER	32



PRUEBA DE HABILIDADES PRACTICAS CCNA

INTRODUCCIÓN

La prueba de habilidades practica que en este trabajo se presenta, tiene como finalidad dar solución a dos escenarios diferentes sobre problemáticas en telecomunicaciones, poniendo a prueba las habilidades de los futuros ingenieros frente a situaciones que se pueden llegar a presentar en el ejercicio de su carrera como pueden ser: iniciación de dispositivos de red, diseñar una red, configurar routers, servidores, switches, suministrar códigos de seguridad, direccionamientos IP, control de acceso, entre otros.

Además debe estar en la capacidad de solucionar problemas y encontrar soluciones a las diversas dificultades que se presentan mientras se construye el código, con las diferentes exigencias que pide la prueba de habilidades práctica, al finalizar los ejercicios, debe estar en la capacidad de redactar un informe detallado de su trabajo, haciendo uso de las herramientas aprendidas durante el Diplomado en Cisco.

Objetivos

General

Implementar todos los conocimientos adquiridos durante el Diplomado de Cisco para la resolución de problemas en telecomunicaciones, usando habilidades prácticas y teóricas que se viven desde la experiencia.

Específicos

- Solucionar problemas de telecomunicaciones, usando las herramientas adquiridas en el Diplomado
- Identificar las posibles soluciones e identificar cual es la más viable
- Categorizar los dispositivos a utilizar en el proyecto Para la solución de una situación
- Crear la configuración de enrutamiento
- Configurar las listas de control de acceso
- Configurar routers, servidores, switches,
- Comprobar la red instalada
- Seguir los parámetros que exige la solución de la guía

1 Escenario 1

Una empresa posee sucursales distribuidas en las ciudades de Bogotá, Medellín y Cali en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red

1.1 DESARROLLO:

Se inicia con la configuración básica, se construye la topología, con los requerimientos de la empresa.

1.2 TOPOLOGIA

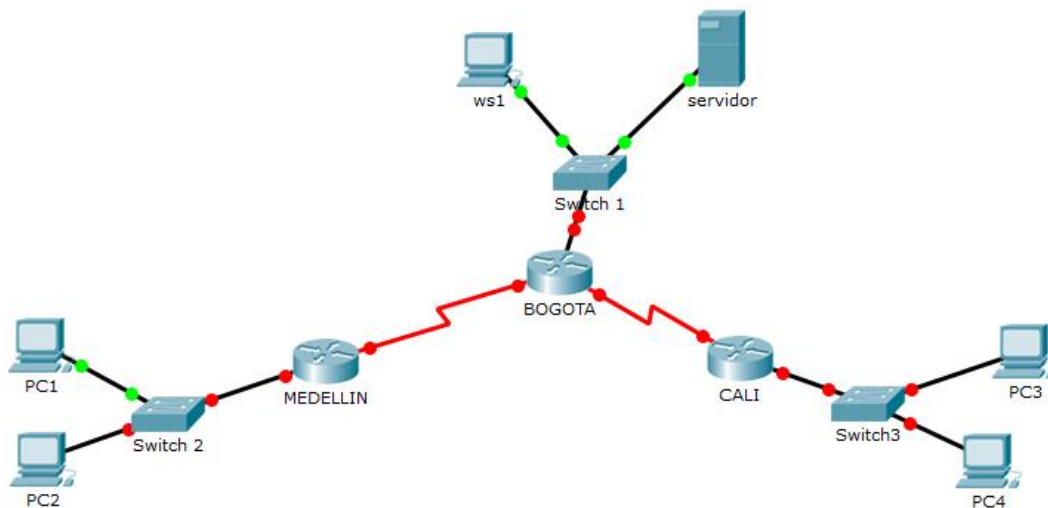
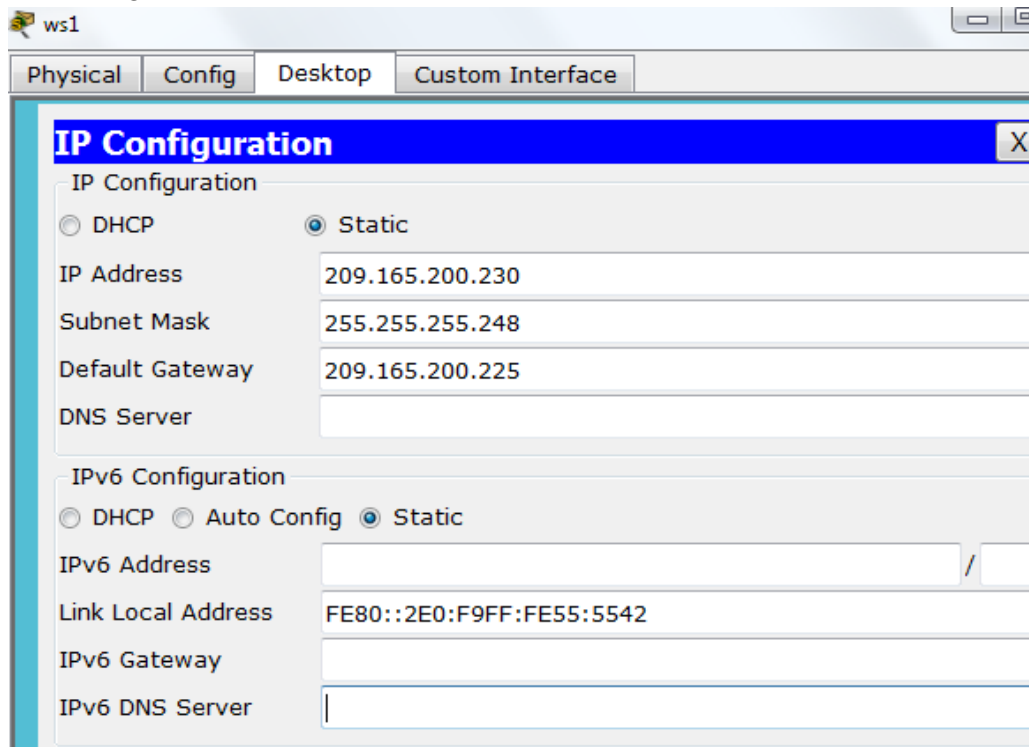


FIGURA 1 TOPOLOGIA

1.3 PARTE 1: ASIGNACIÓN DE DIRECCIONAMIENTO IP.

- ✓ se asigna IP a cada uno de los switch, servidor, PC y routers, tal como se ve en las graficas

1.3.1



The screenshot shows the 'IP Configuration' window for a PC named 'ws1'. The window has tabs for 'Physical', 'Config', 'Desktop', and 'Custom Interface'. The 'Config' tab is selected. Under 'IP Configuration', the 'Static' radio button is selected. The fields are filled with the following values:

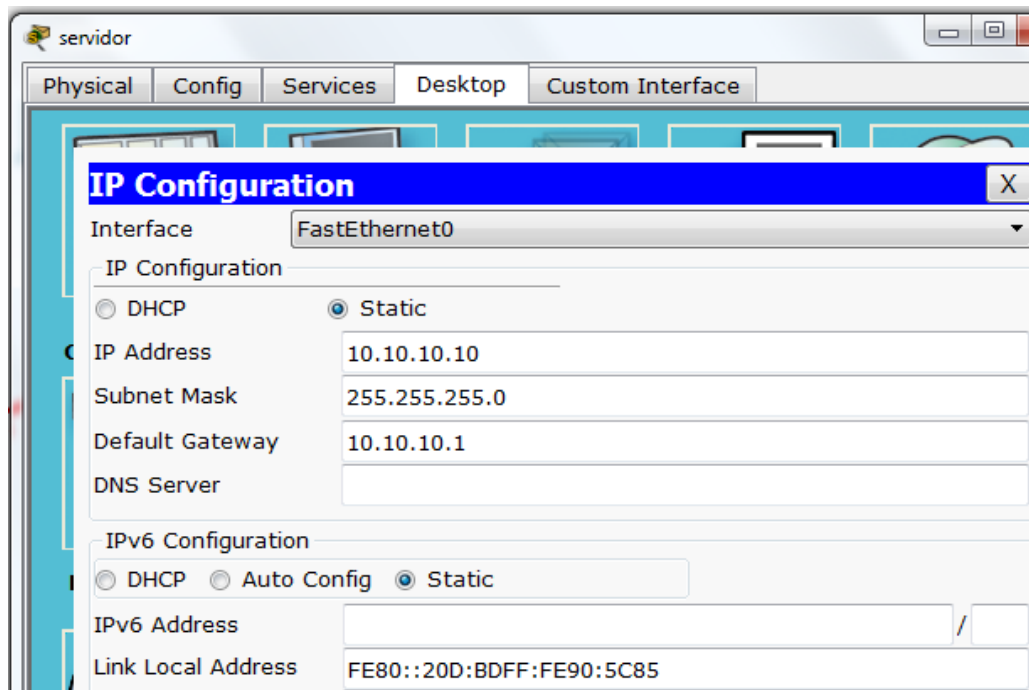
Field	Value
IP Address	209.165.200.230
Subnet Mask	255.255.255.248
Default Gateway	209.165.200.225
DNS Server	

Under 'IPv6 Configuration', the 'Static' radio button is selected. The fields are filled with the following values:

Field	Value
IPv6 Address	
Link Local Address	FE80::2E0:F9FF:FE55:5542
IPv6 Gateway	
IPv6 DNS Server	

FIGURA2 INTERNET PC

1.3.2



The screenshot shows the 'IP Configuration' window for a server named 'servidor'. The window has tabs for 'Physical', 'Config', 'Services', 'Desktop', and 'Custom Interface'. The 'Config' tab is selected. Under 'IP Configuration', the 'Static' radio button is selected. The fields are filled with the following values:

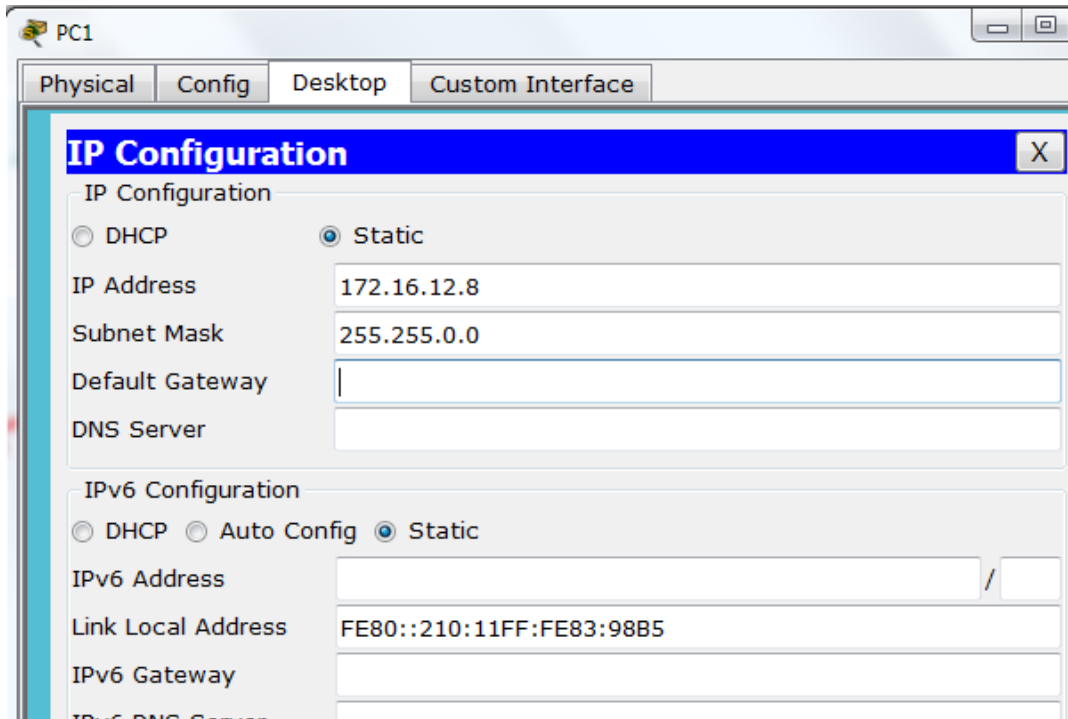
Field	Value
Interface	FastEthernet0
IP Address	10.10.10.10
Subnet Mask	255.255.255.0
Default Gateway	10.10.10.1
DNS Server	

Under 'IPv6 Configuration', the 'Static' radio button is selected. The fields are filled with the following values:

Field	Value
IPv6 Address	
Link Local Address	FE80::20D:BDFF:FE90:5C85

FIGURA 3 WEB SERVER

1.3.3



PC1

Physical Config Desktop Custom Interface

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address: 172.16.12.8

Subnet Mask: 255.255.0.0

Default Gateway:

DNS Server:

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address: /

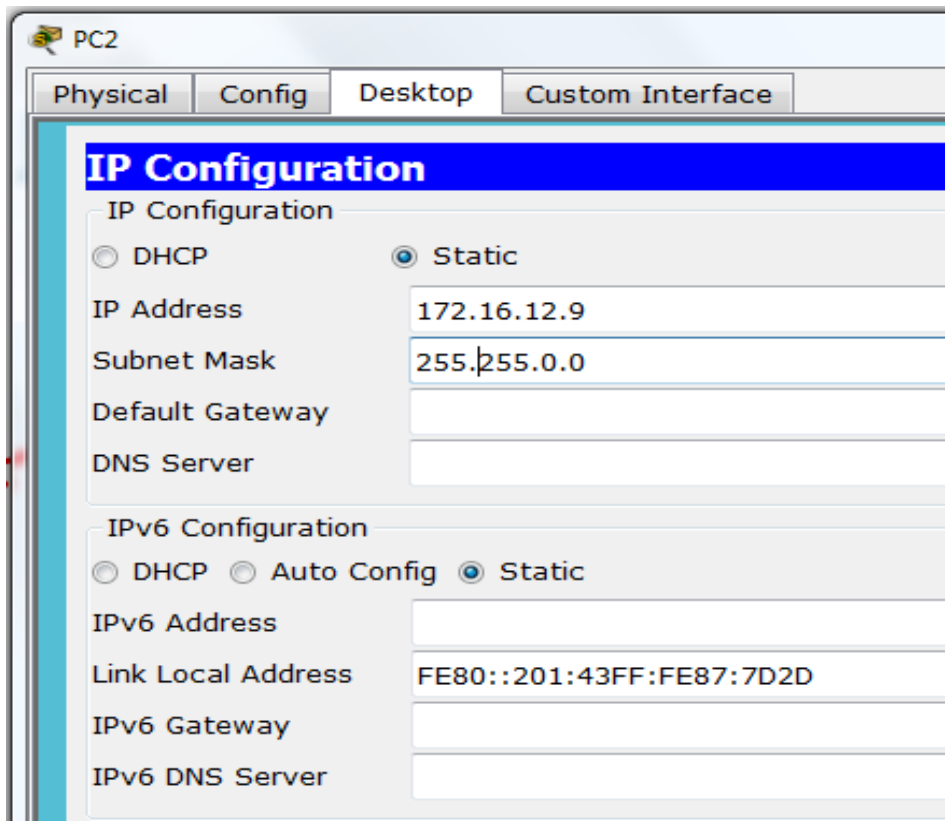
Link Local Address: FE80::210:11FF:FE83:98B5

IPv6 Gateway:

IPv6 DNS Server:

FIGURA 4 PC-1

1.3.4



PC2

Physical Config Desktop Custom Interface

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address: 172.16.12.9

Subnet Mask: 255.255.0.0

Default Gateway:

DNS Server:

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address:

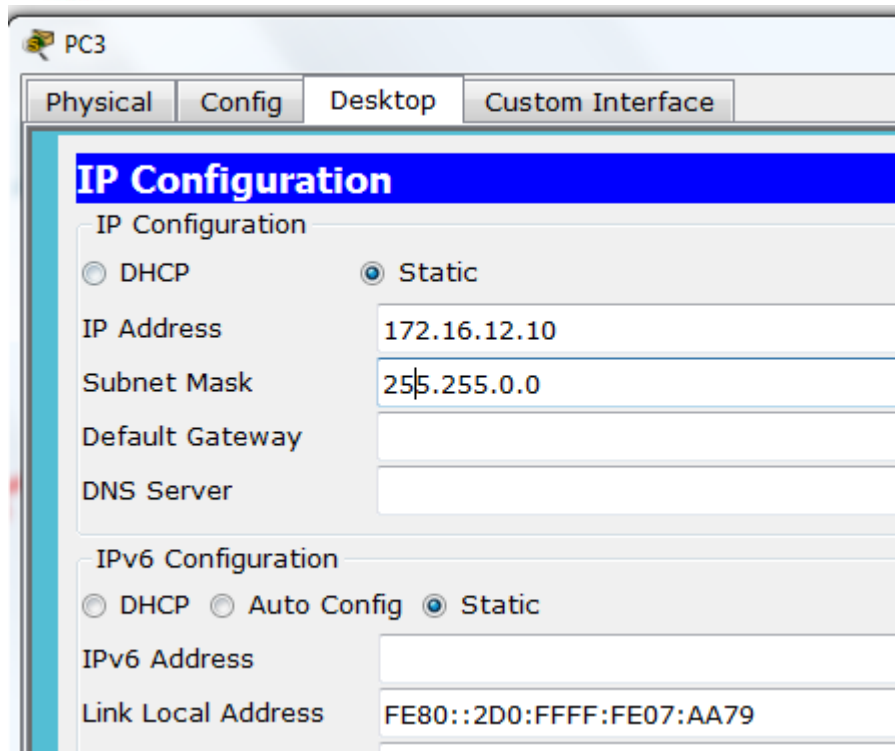
Link Local Address: FE80::201:43FF:FE87:7D2D

IPv6 Gateway:

IPv6 DNS Server:

Figura 5 PC-2

1.3.5



PC3

Physical Config Desktop Custom Interface

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address 172.16.12.10

Subnet Mask 255.255.0.0

Default Gateway

DNS Server

IPv6 Configuration

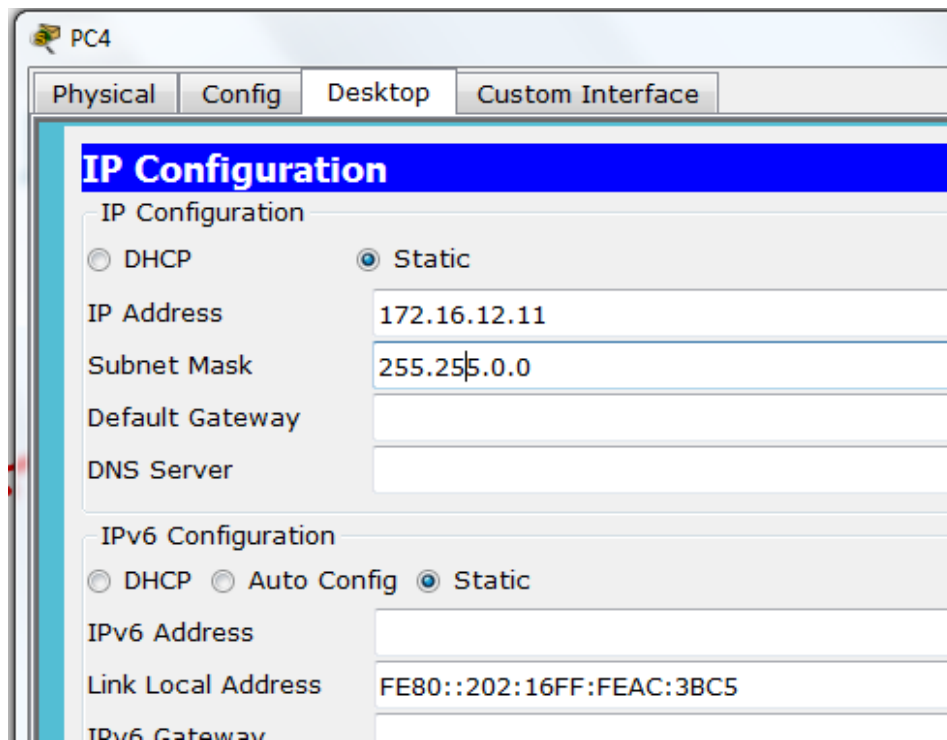
☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address

Link Local Address FE80::2D0:FFFF:FE07:AA79

Figura 6 PC-3

1.3.6



PC4

Physical Config Desktop Custom Interface

IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address 172.16.12.11

Subnet Mask 255.255.0.0

Default Gateway

DNS Server

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address

Link Local Address FE80::202:16FF:FEAC:3BC5

IPv6 Gateway

FIGURA 7 PC-4

1.4 PARTE 2: CONFIGURACIÓN BÁSICA.

1.5 Configuración Básica De Dispositivos

Aplicar a cada Router y Switch de la topología, las siguientes configuraciones básicas;

- R1: nombrarlo "Medellín"
- R2: nombrarlo "Bogotá"
- R3: nombrarlo "Cali"
- S1: nombrarlo "Switch1"
- S2: nombrarlo "Switch2"
- S3: nombrarlo "Switch3"
- ✓ Exec Password: class
- ✓ Console Access Password: cisco
- ✓ Telnet Access Password: cisco
- ✓ Encriptar contraseñas
- ✓ MOTD banner: Prohibido personal no autorizado
- ✓ A cada Switch deshabilitar DNS lookup

A. TABLA:

	R1	R2	R3
Nombre de Host	MEDELLIN	BOGOTA	CALI
Dirección de Ip en interfaz Serial 0/0	192.268.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 0/1	192.168.1.50	192.168.1.130	192.168.1.43
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	Eigrp	Eigrp	Eigrp
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

FIGURA 8 TABLA DE CONFIGURACION BASICA

a. Después de cargada la configuración en los dispositivos, verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

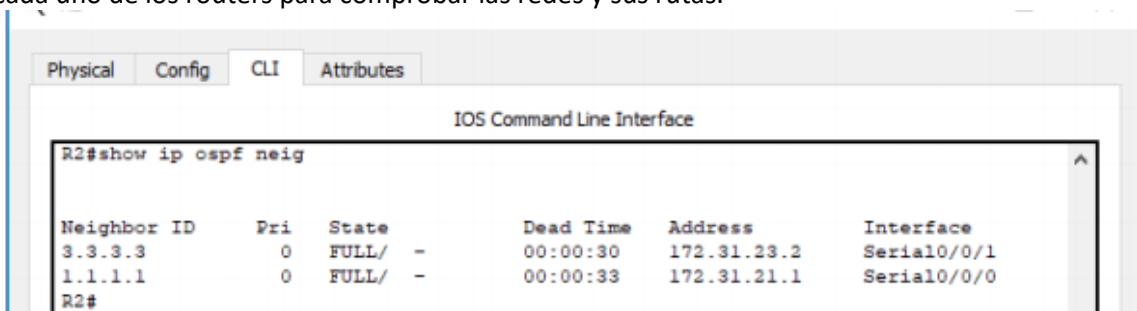


FIGURA 9 VERIFICACIÓN ENRUTAMIENTO

b. Realizar un diagnóstico de vecinos usando el comando cdp.

1.6 D DIAGNOSTICO DE VECINOS COMANDO CDP:

- c. switch2#show cdp ne
- d. switch2#show cdp neighbors

- e. capability codes: R - Router, T - Trans Bridge, B - Source route bridge
- f. s - switch, H - host, I - ICMP, r - repeater, P - Phone
- g. Device ID Local interface holdtime capability platform port ID
- h. switch1 fas 0/1 12 2950 Fas 0/2
- i. switch2#show cdp neighbors det
- j. switch2#show cdp neighbors detail
- k.
- l. Device ID: Switch1
- m. entry address : 10.10.1.1
- n. platform: cisco 2950, capabilities: switch
- o. interface: fastEthernet0/1, port ID (outgoing port): fastEthernet0/2
- p. holdtime: 121
- q.
- r. version:
- s. cisco internetwork operating system software
- t. IOS (tm) c2950 software (c2950-I6Q4L2-M), version 12.1(22)EA4, release software(fcl)
- u. advertisement version:2
- v. duplex: full
- w. E. realizar prueba de conectividad usando comando ping
- x. PC>ping 10.10.1.1
- y.
- z. pinging 10.10.1.1 with 32 bytes of data:
- aa.
- bb. reply from 10.10.1.1: bytes=32 time=31ms TTL=255
- cc. reply from 10.10.1.1: bytes=32 time=31ms TTL=255
- dd. reply from 10.10.1.1: bytes=32 time=31ms TTL=255
- ee. reply from 10.10.1.1: bytes=32 time=31ms TTL=255
- ff.
- gg. Ping statistics for 10.10.1.1:
- hh. packets: sent = 4, received = 4, lost = 0 (0% loss),
- ii. approximate round trip times in milli-seconds:
- jj. minimum = 15ms, maximum = 31ms, average = 27ms

- c. Realizar una prueba de conectividad en cada tramo de la ruta usando Ping.

1.7 PRUEBA DE CONECTIVIDAD CON PING

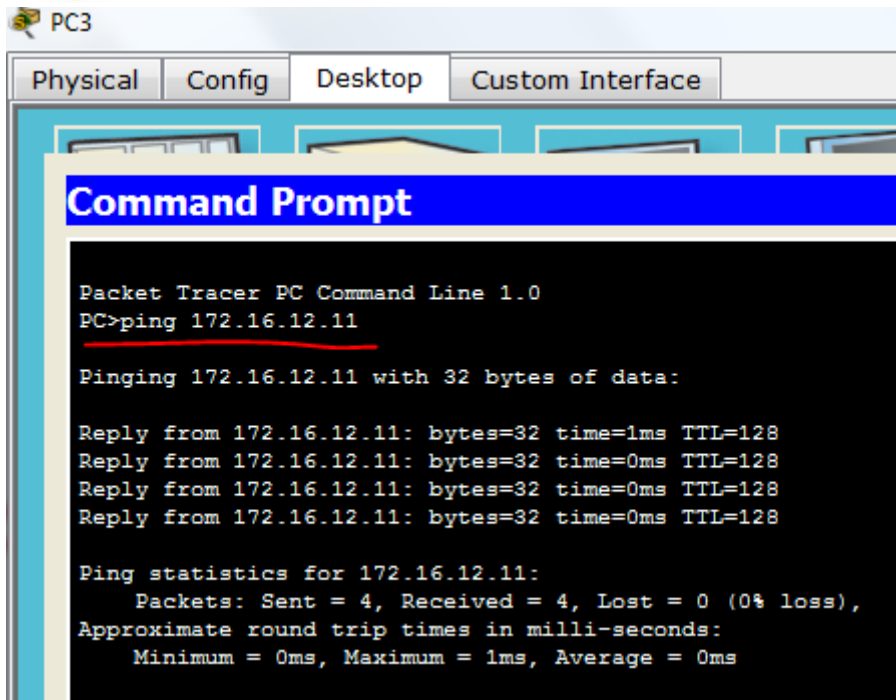


Figura 10 pin PC 3 -medellin

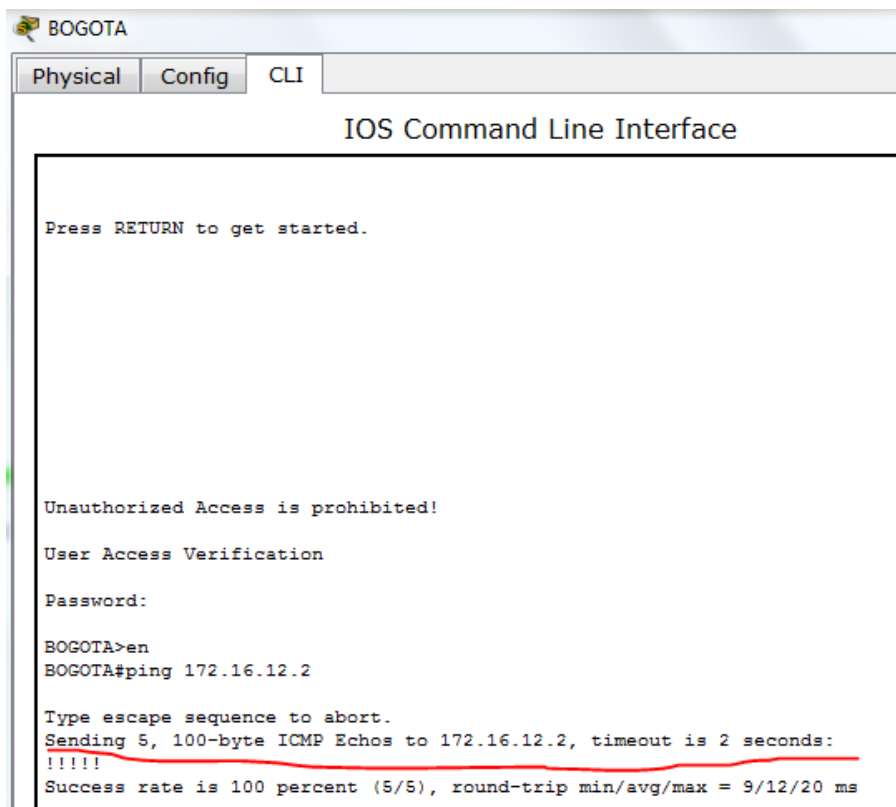


FIGURA 11 PING BOGOTA- MEDELLIN
Se hace ping Bogota a servidor

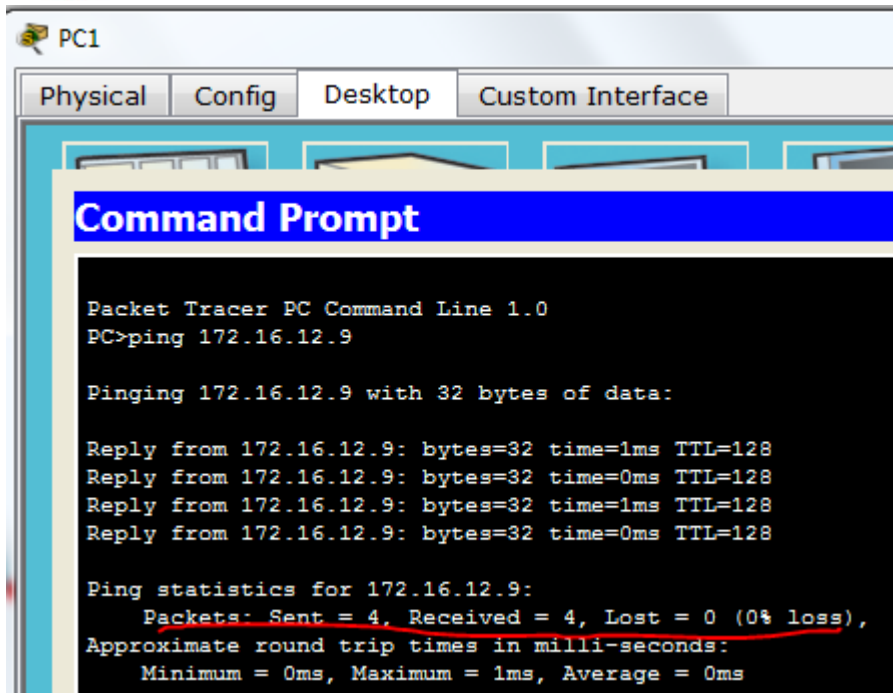


figura 12 ping Bogot- SERVIDOR

PARTE 3

.1.8 CONFIGURACIÓN DE DISPOSITIVOS DE ENRUTAMIENTO:

En las siguientes gráficas, se puede observar las configuraciones que se le dieron a cada uno de los routers, y el código.

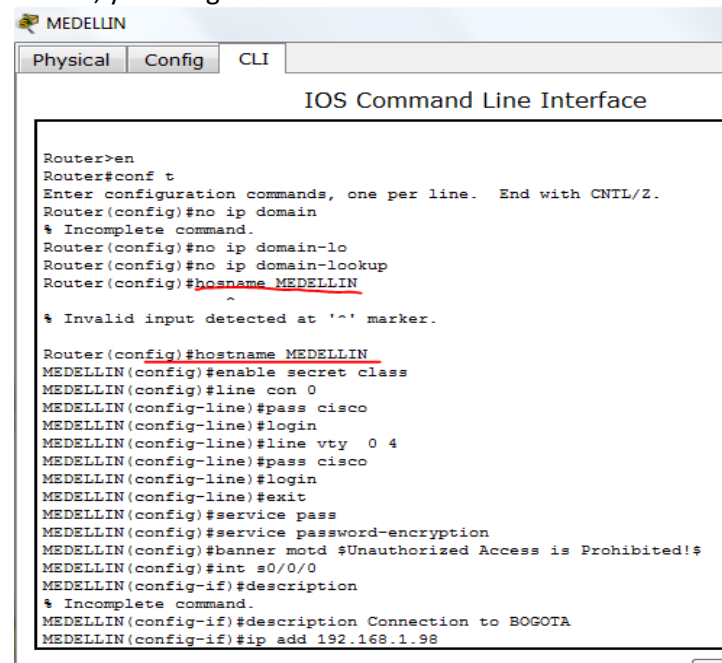


FIGURA 13 DISPOSITIVO DE ENRUTAMIENTO MEDELLIN

BOGOTA

Physical	Config	CLI
----------	--------	-----

IOS Command Line Interface

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-look
Router(config)#no ip domain-lookup
Router(config)#host BOGOTA
BOGOTA(config)#line con 0
BOGOTA(config-line)#pass cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#line vty 0 4
BOGOTA(config-line)#pass cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#service
% Incomplete command.
BOGOTA(config)#service pass
BOGOTA(config)#service password-encryption
^
% Invalid input detected at '^' marker.

BOGOTA(config)#service password-encryption
^
% Invalid input detected at '^' marker.

BOGOTA(config)#service password-encryption
BOGOTA(config)#banner motd #Unauthorized Access is prohibited!#
BOGOTA(config)#int s0/0/0
BOGOTA(config-if)#descrip Connection to MEDELLIN
BOGOTA(config-if)#ip add 192.268.1.99 255.255.255.252
  
```

FIGURA 14 DISPOSITIVO DE ENRUTAMIENTO BOGOTA

CALI

Physical	Config	CLI
----------	--------	-----

IOS Command Line Interface

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-look
Router(config)#no ip domain-lookup
Router(config)#host CALI
CALI(config)#enable secret class
CALI(config)#line con 0
CALI(config-line)#pass cisco
CALI(config-line)#login line vty 0 4
^
% Invalid input detected at '^' marker.

CALI(config-line)#login
CALI(config-line)#line vty 0 4
CALI(config-line)#pass cisco
CALI(config-line)#login
CALI(config-line)#exit
CALI(config)#service
% Incomplete command.
CALI(config)#service pass
CALI(config)#service password-encryption
CALI(config)#banner motd #Unauthorized Access is Prohibited!#
CALI(config)#int
% Incomplete command.
CALI(config)#conf if
%Invalid hex value
CALI(config)#int s0/0/1
CALI(config-if)#descrip Connection to BOGOTA
CALI(config-if)#ip add 192.168.1.98 255.255.255.252
  
```

FIGURA 15 DISPOSITIVO DE ENRUTAMIENTO CALI

1.9 Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.

Se Habilita el proceso de routing EIGRP en cada router con el número de AS 1. Se muestra la configuración para el **R1**. (Medellín)

```
Medellín(config)# router eigrp 1
```

Observaciones: en la actualidad, Packet Tracer no permite la configuración de una ID de router EIGRP

a. Verificar si existe vecindad con los routers configurados con EIGRP.

En cada router, se configura EIGRP para comunicar las subredes específicas enlazadas directamente. Como ejemplo tenemos la configuración para el **R1**. (Medellín)

```
Medellin(config-router)#network 172.16.1.0.0.0.0.255
```

```
Medellin(config-router)#network 172.16.3.0.0.0.0.3
```

```
Medellin(config-router)#network 192.168.10.4.0.0.0.3
```

Los tres routers deberán tener dos vecinos en la lista. El resultado para el **R1 (Medellín)** debe ser equivalente a lo siguiente:

```
IP-EIGRP neighbors for process 1
```

H	Address	interface	hold	uptime	SRTT	rto	Q	SEGO
0	172.16.3.2	Se0/0/0	14	00:25:05	40	1000	0	28
1	192.168.10.6	Se0/0/1	12	00:13:29	40	1000	0	31

b. Realizar la comprobación de las tablas de enrutamiento en cada uno de los routers para verificar cada una de las rutas establecidas.

1.9 PARTE 3. PROTOCOLO DE ENRUTAMIENTO

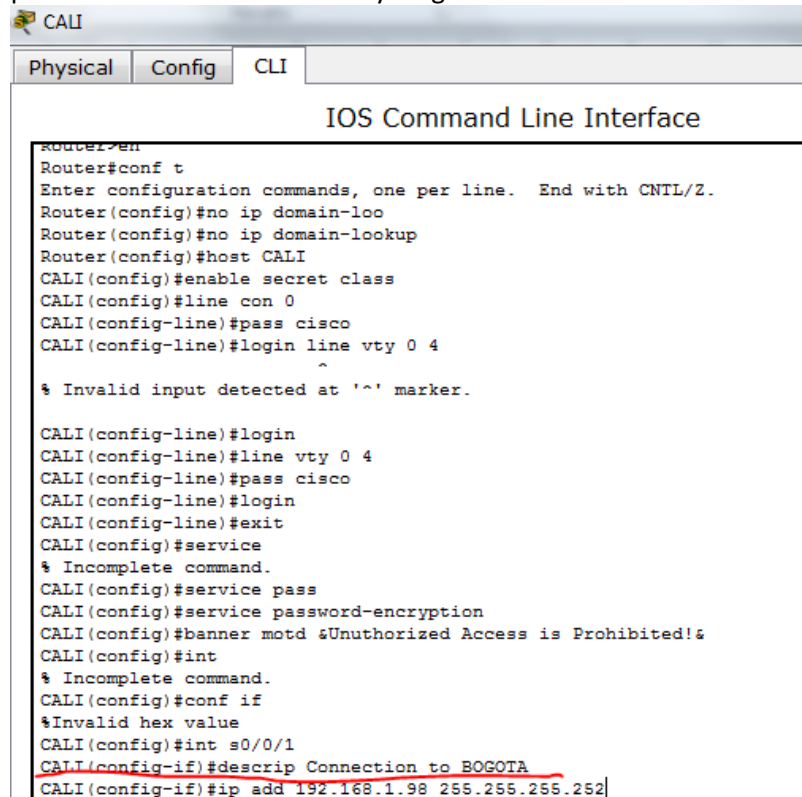
Configuration	Specification
Router ID R1	1.1.1.1
Router ID R2	2.2.2.2
Router ID R3	3.3.3.3
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en:	128 Kb/s
Ajustar el costo en la métrica de S0/0 a:	7500

FIGURA 16 PROTOCOLO ENRUTAMIENTO

Dispositivo	destino	Dirección IP	Mascara de sub red	Gateway predeterminado
Router 1	Medellín	192.268.199	255.255.255.252	2001:DB8:ACAD:12::1/64
Router 2	Bogotá	192.168.1.98	255.255.255.252	2001:DB8:ACAD:12::2/64
Router 3	Cali	192.168.1.131	255.255.255.252	2001:DB8:ACAD:12::3/64

FIGURA 17 COMPROBACION DE ENRUTAMIENTO

c. Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad entre sí. Realizar esta prueba desde un host de la red LAN del router CALI, primero a la red de MEDELLIN y luego al servidor.

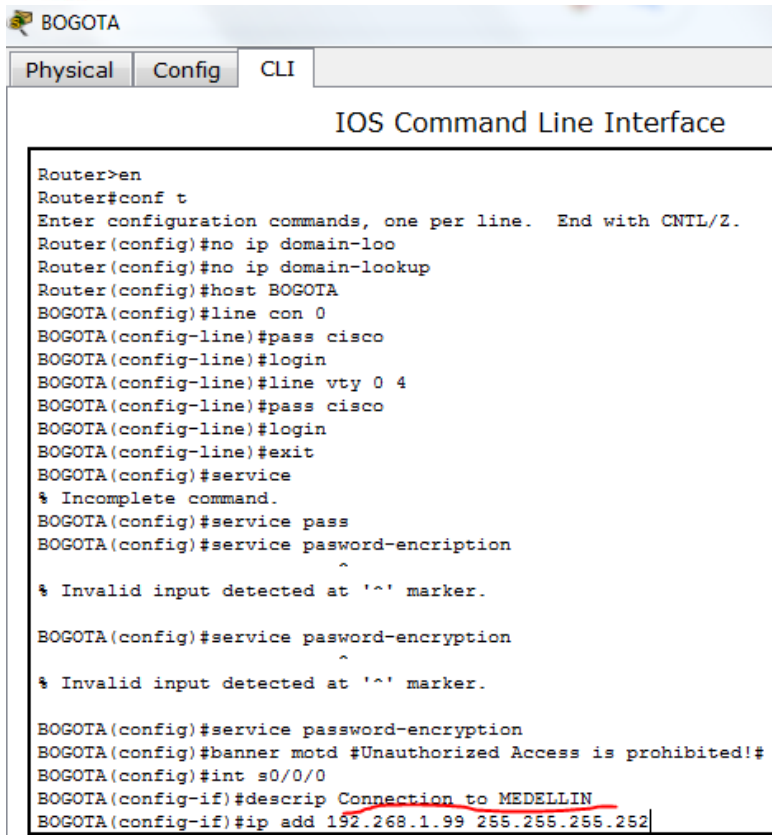


```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-look
Router(config)#no ip domain-lookup
Router(config)#host CALI
CALI(config)#enable secret class
CALI(config)#line con 0
CALI(config-line)#pass cisco
CALI(config-line)#login line vty 0 4
^
% Invalid input detected at '^' marker.

CALI(config-line)#login
CALI(config-line)#line vty 0 4
CALI(config-line)#pass cisco
CALI(config-line)#login
CALI(config-line)#exit
CALI(config)#service
% Incomplete command.
CALI(config)#service pass
CALI(config)#service password-encryption
CALI(config)#banner motd &Unauthorized Access is Prohibited!&
CALI(config)#int
% Incomplete command.
CALI(config)#conf if
%Invalid hex value
CALI(config)#int s0/0/1
CALI(config-if)#descrip Connection to BOGOTA
CALI(config-if)#ip add 192.168.1.98 255.255.255.252
  
```

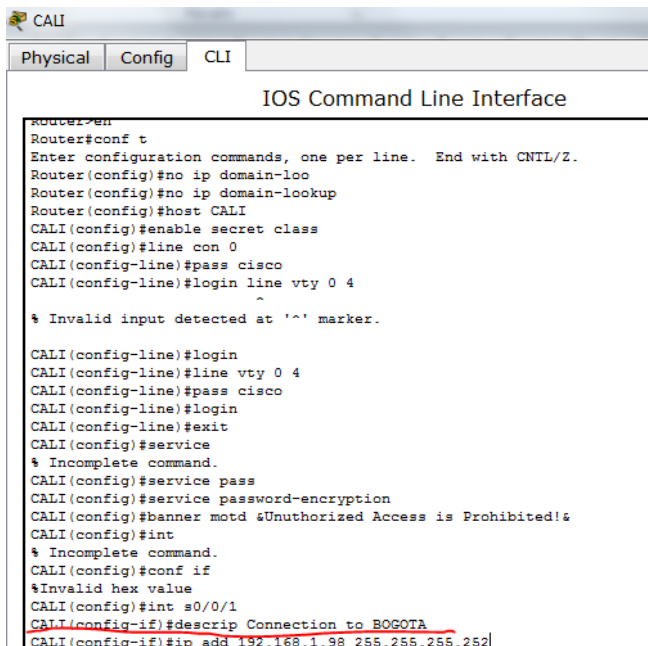
FIGURA 18 configuración de dispositivos de enrutamiento R1



```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-look
Router(config)#no ip domain-lookup
Router(config)#host BOGOTA
BOGOTA(config)#line con 0
BOGOTA(config-line)#pass cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#line vty 0 4
BOGOTA(config-line)#pass cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#service
% Incomplete command.
BOGOTA(config)#service pass
BOGOTA(config)#service password-encryption
BOGOTA(config)#service password-encryption
BOGOTA(config)#banner motd #Unauthorized Access is prohibited!#
BOGOTA(config)#int s0/0/0
BOGOTA(config-if)#descrip Connection to MEDELLIN
BOGOTA(config-if)#ip add 192.268.1.99 255.255.255.252
  
```

FIGURA 18 configuración de dispositivos de enrutamiento R2

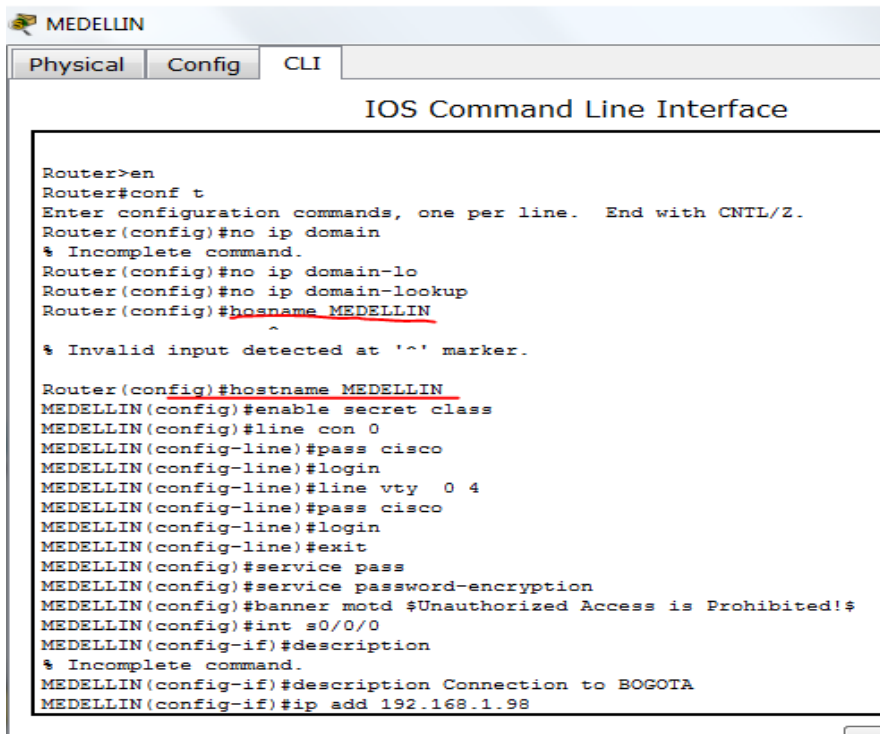


```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-look
Router(config)#no ip domain-lookup
Router(config)#host CALI
CALI(config)#enable secret class
CALI(config)#line con 0
CALI(config-line)#pass cisco
CALI(config-line)#login line vty 0 4
CALI(config-line)#login
CALI(config-line)#line vty 0 4
CALI(config-line)#pass cisco
CALI(config-line)#login
CALI(config-line)#exit
CALI(config)#service
% Incomplete command.
CALI(config)#service pass
CALI(config)#service password-encryption
CALI(config)#banner motd #Unauthorized Access is Prohibited!#
CALI(config)#int
% Incomplete command.
CALI(config)#conf if
%Invalid hex value
CALI(config)#int s0/0/1
CALI(config-if)#descrip Connection to BOGOTA
CALI(config-if)#ip add 192.168.1.98 255.255.255.252
  
```

FIGURA 19 configuración de dispositivos de enrutamiento R3

- 1.10 Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad entre sí. Realizar esta prueba desde un host de la red LAN del router CALI, primero a la red de MEDELLIN y luego al servidor.



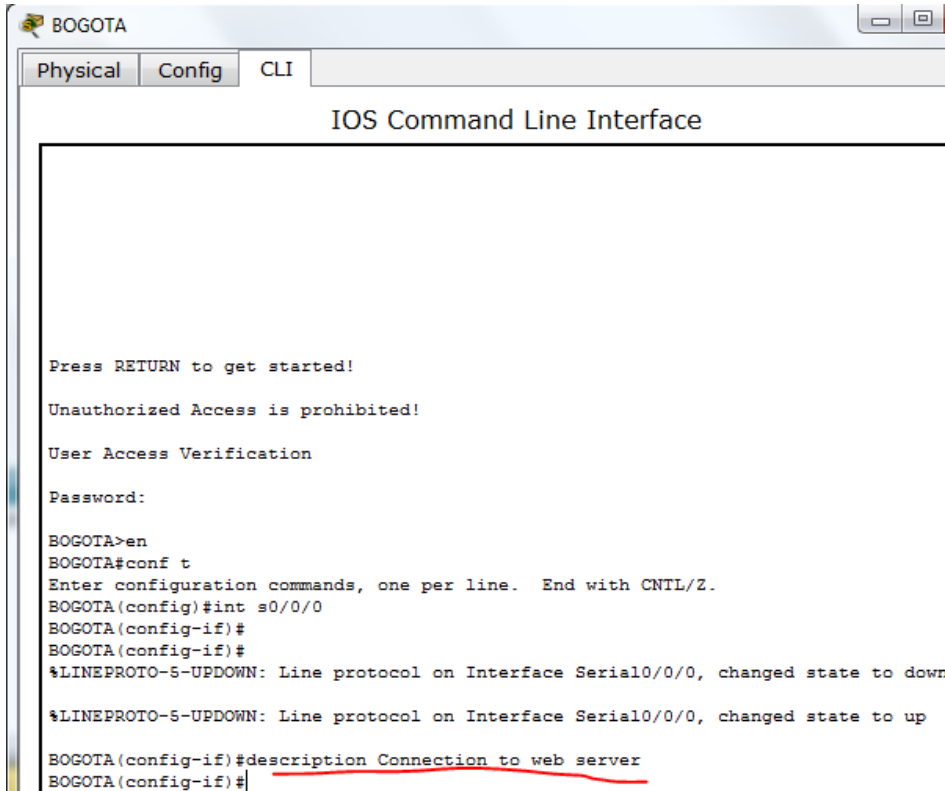
```

MEDELLIN
Physical Config CLI
IOS Command Line Interface

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain
% Incomplete command.
Router(config)#no ip domain-lo
Router(config)#no ip domain-lookup
Router(config)#hostname MEDELLIN
^
% Invalid input detected at '^' marker.

Router(config)#hostname MEDELLIN
MEDELLIN(config)#enable secret class
MEDELLIN(config)#line con 0
MEDELLIN(config-line)#pass cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#line vty 0 4
MEDELLIN(config-line)#pass cisco
MEDELLIN(config-line)#login
MEDELLIN(config-line)#exit
MEDELLIN(config)#service pass
MEDELLIN(config)#service password-encryption
MEDELLIN(config)#banner motd $Unauthorized Access is Prohibited!$
MEDELLIN(config)#int s0/0/0
MEDELLIN(config-if)#description
% Incomplete command.
MEDELLIN(config-if)#description Connection to BOGOTA
MEDELLIN(config-if)#ip add 192.168.1.98
  
```

FIGURA 20 PUNTOS DE CONECTIVIDAD



```

BOGOTA
Physical Config CLI
IOS Command Line Interface

Press RETURN to get started!

Unauthorized Access is prohibited!

User Access Verification

Password:

BOGOTA>en
BOGOTA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#int s0/0/0
BOGOTA(config-if)#
BOGOTA(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up

BOGOTA(config-if)#description Connection to web server
BOGOTA(config-if)#
  
```

FIGURA 21 VERIFICACIÓN DE ENRUTAMIENTO DE ROUTERS CON EL SERVIDOR

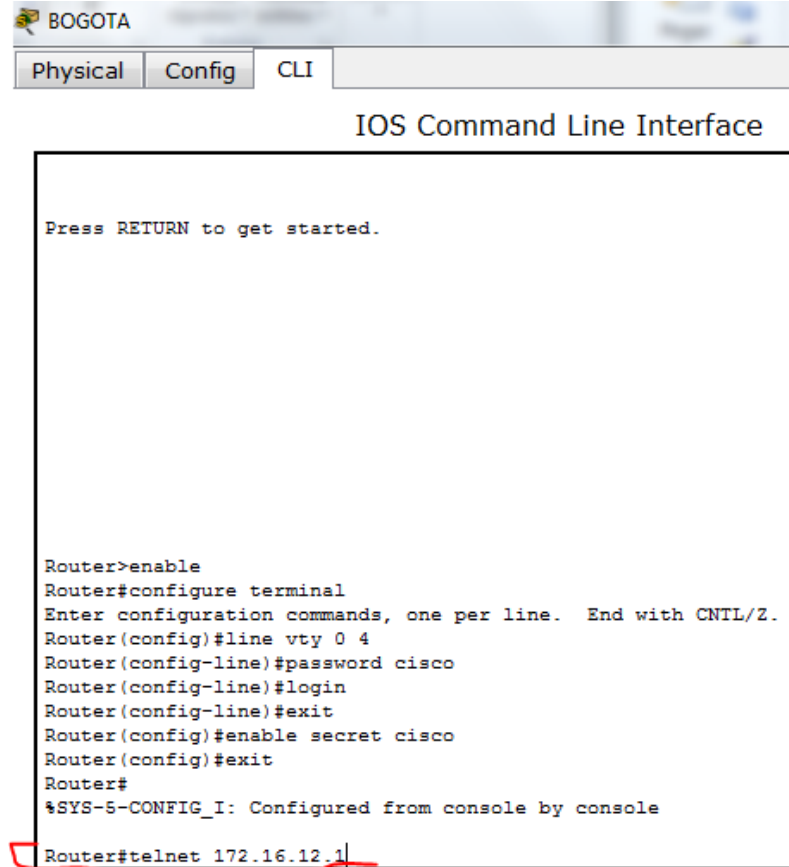
PARTE 4

1.11 CONFIGURACION DE LAS LISTAS DE CONTROL DE ACCESO

En este momento cualquier usuario de la red tiene acceso a todos sus dispositivos y estaciones de trabajo. El jefe de redes le solicita implementar seguridad en la red. Para esta labor se decide configurar listas de control de acceso (ACL) a los routers.

Las condiciones para crear las ACL son las siguientes:

- a. Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red.



```

BOGOTA
Physical Config CLI
IOS Command Line Interface

Press RETURN to get started.

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line vty 0 4
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#enable secret cisco
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#telnet 172.16.12.1
  
```

FIGURA 21 CONFIGURACION TELNET

- b. El equipo WS1 y el servidor se encuentran en la subred de administración. Solo el servidor de la subred de administración debe tener acceso a cualquier otro dispositivo en cualquier parte de la red.
- c. Las estaciones de trabajo en las LAN de MEDELLIN y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor:

A continuación, se realizará unos pasos de ACL extendida en R2 para proteger la red del tráfico que genera el acceso a internet.

Se configura las listas de control de acceso ACL a los routers con el siguiente código controlar el acceso:

R2#conf t



```
CALI(config)#access-list 100 permit tcp any host 209.165.200.229 eq www
CALI(config)#access-list 100 permit icmp any any echo-reply
CALI(config)#int f0/0
(config-if)#ip access-group 100 in
R2(config-if)#exit
```

Habilitamos el router para establecer conexión TELNET y tener acceso a cualquier conexión de la red

```
MEDELLIN1(config)#ip nat inside source list HOST interface s0/0 overload
MEDELLIN1(config)#int s0/0
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/2
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/3
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#exit
MEDELLIN1#show ip nat
translation
```

```
CALI>en
CALI #conf t
CALI (config)#ip access-list standard HOST
CALI (config-std-nacl)#permit 172.29.0.0 0.0.0.255 CALI
(config)#ip nat inside source list HOST interface s0/0
overload
CALI(config)#int s0/0
CALI(config-if)#ip nat outside
CALI(config-if)#exit
CALI| (config)#int s0/1
CALI(config-if)#ip nat inside
CALI(config-if)#exit
BOGOTA1(config)#int s0/2 SERVIDOR
SERVIDOR(config-if)#ip nat inside
SERVIDOR (config-if)#exit
SERVIDOR (config)#int s0/3
SERVIDOR (config-if)#ip nat inside
```

SERVIDOR (config-if)#exit
 SERVIDOR (config)#exit
 SERVIDOR #show ip nat translation

1.12 Parte 5: Comprobación de la red instalada.

a. Se debe probar que la configuración de las listas de acceso fue exitosa.

FIGURA

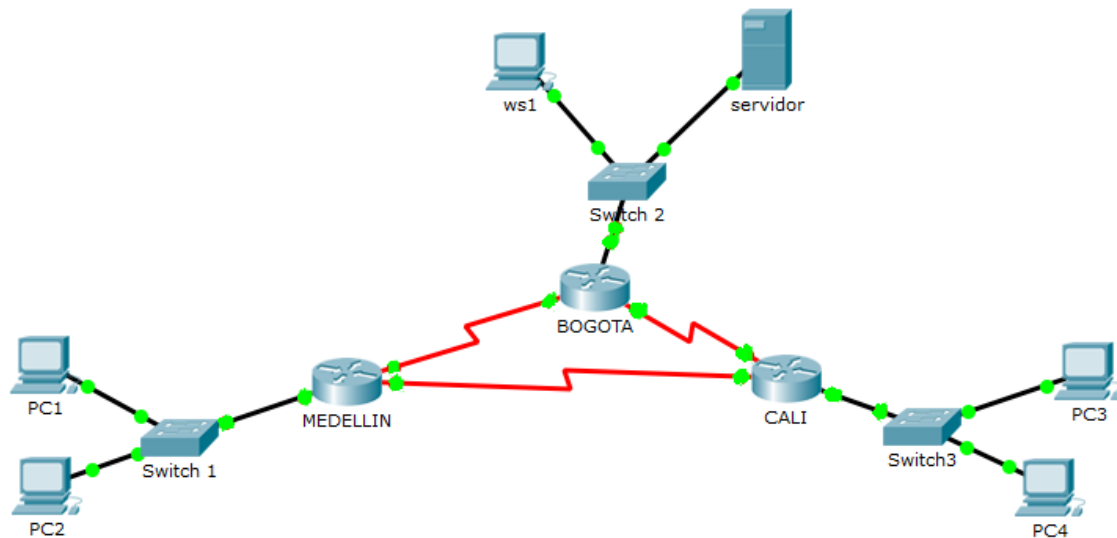


FIGURA23 CONEXIÓN EXITOSA

```
Bogota#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#ip access-list standard ADMIN
Bogota(config-std-nacl)#permit host 172.31.21.1
Bogota(config-std-nacl)#exit
Bogota(config)#line vty 0 4
Bogota(config-line)#access-class ADMIN in
Bogota(config-line)#
```

Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	ok
	WS_1	Router BOGOTA	ok
	Servidor	Router CALI	ok
	Servidor	Router MEDELLIN	ok

TELNET	LAN del Router MEDELLIN	Router CALI	ok
	LAN del Router CALI	Router CALI	ok
	LAN del Router MEDELLIN	Router MEDELLIN	ok
	LAN del Router CALI	Router MEDELLIN	ok
PING	LAN del Router CALI	WS_1	ok
	LAN del Router MEDELLIN	WS_1	ok
	LAN del Router MEDELLIN	LAN del Router CALI	ok
	LAN del Router MEDELLIN	LAN del Router CALI	ok
PING	LAN del Router CALI	Servidor	ok
	LAN del Router MEDELLIN	Servidor	ok
	Servidor	LAN del Router MEDELLIN	ok
	Servidor	LAN del Router CALI	Ok
	Router CALI	LAN del Router MEDELLIN	Ok
	Router MEDELLIN	LAN del Router CALI	ok

FIGURA 22 COMPROBACION DE LA RED

2 ESCENARIO 2.

Una empresa tiene la conexión a internet en una red Ethernet, lo cual deben adaptarlo para facilitar que sus routers y las redes que incluyen puedan, por esa vía, conectarse a internet, pero empleando las direcciones de la red LAN original.

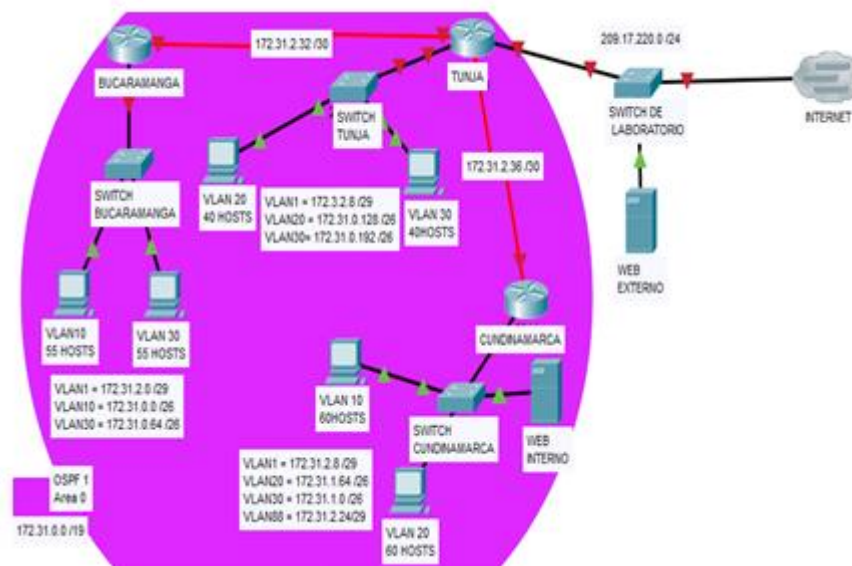


FIGURA 24 CONEXIÓN ESCENARIO 2 INTERNET EN UNA ETHERNET

2.1 Desarrollo

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:
 - Configuración básica.

2.2 TOPOLOGIA

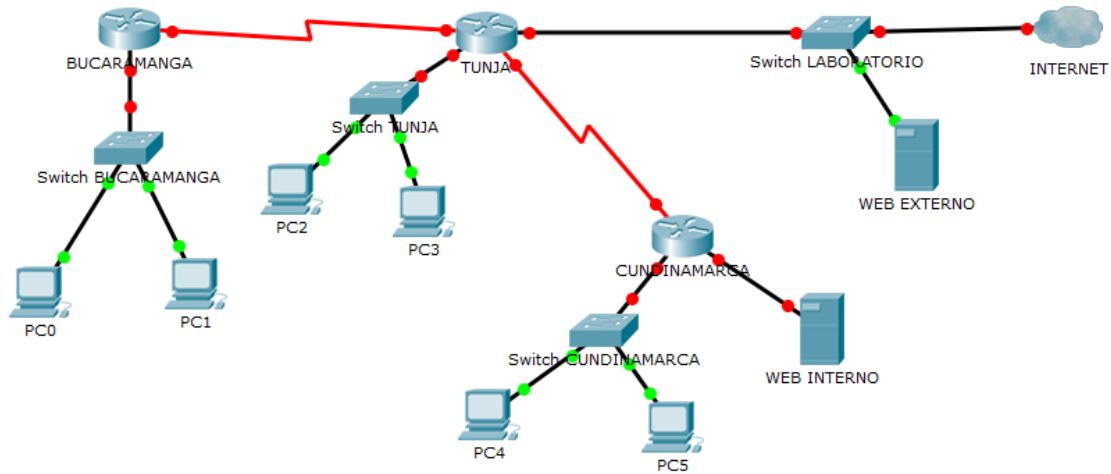


FIGURA 25 TOPOLOGIA

2.3 Cifrado de contraseñas.

```

BUCARAMANGA
Physical Config CLI
IOS Command Line Interface


Press RETURN to get started!

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-look
Router(config)#no ip domain-lookup
Router(config)#host BUCARAMANGA
Router(config)#host BUCARAMANGA
^
% Invalid input detected at '^' marker.

Router(config)#host BUCARAMANGA
BUCARAMANGA(config)#line con 0
BUCARAMANGA(config-line)#pass cisco
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#line vty 0 4
BUCARAMANGA(config-line)#pass cisco
BUCARAMANGA(config-line)#login
BUCARAMANGA(config-line)#exit
BUCARAMANGA(config)#
  
```

FIGURA 26 CONFIGURACION BASICA

 TUNJA

Physical Config CLI

IOS Command Line Interface


```

User Access Verification

Password:

BUCARAMANGA>en
BUCARAMANGA#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#exit
BUCARAMANGA#
%SYS-5-CONFIG_I: Configured from console by console
conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
BUCARAMANGA(config)#no ip domain-look
BUCARAMANGA(config)#no ip domain-lookup
BUCARAMANGA(config)#host TUNJA
TUNJA(config)#line con 0
TUNJA(config-line)#pass cisco
TUNJA(config-line)#login
TUNJA(config-line)#line vty 0 4
TUNJA(config-line)#pass cisco
TUNJA(config-line)#login
TUNJA(config-line)#exit
TUNJA(config)#
  
```

FIGURA 27 CONFIGURACION BASICA TUNJA

 CUNDINAMARCA

Physical Config CLI

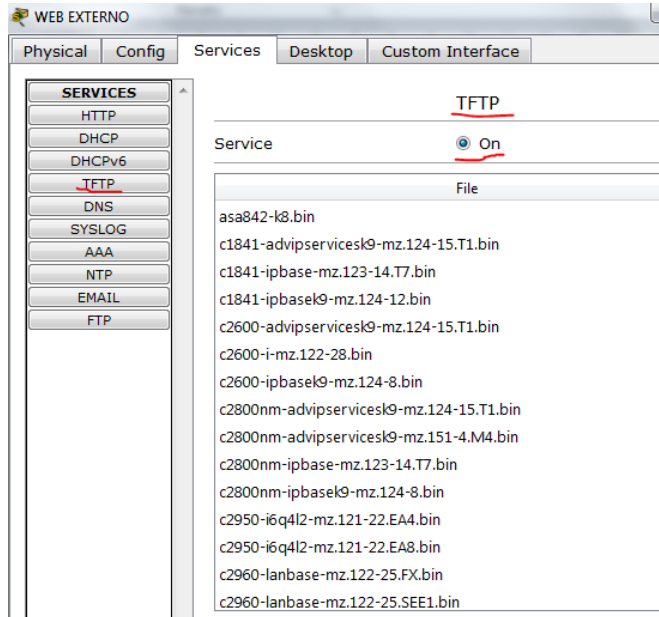
IOS Command Line Interface

```

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-look
Router(config)#no ip domain-lookup
Router(config)#host CUNDINAMARCA
CUNDINAMARCA(config)#line con 0
CUNDINAMARCA(config-line)#pass cisco
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#line vty 0 4
CUNDINAMARCA(config-line)#pass cisco
CUNDINAMARCA(config-line)#login
CUNDINAMARCA(config-line)#exit
  
```

FIGURA 28 CONFIGURACION CUNDINAMARCA

2.4 Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.



2.5 El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca

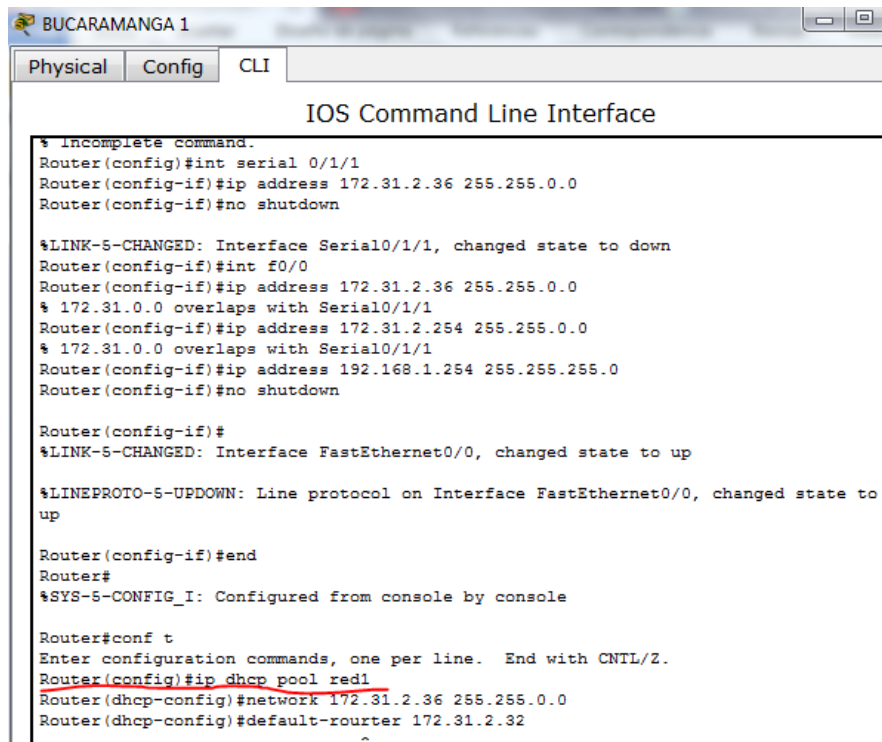
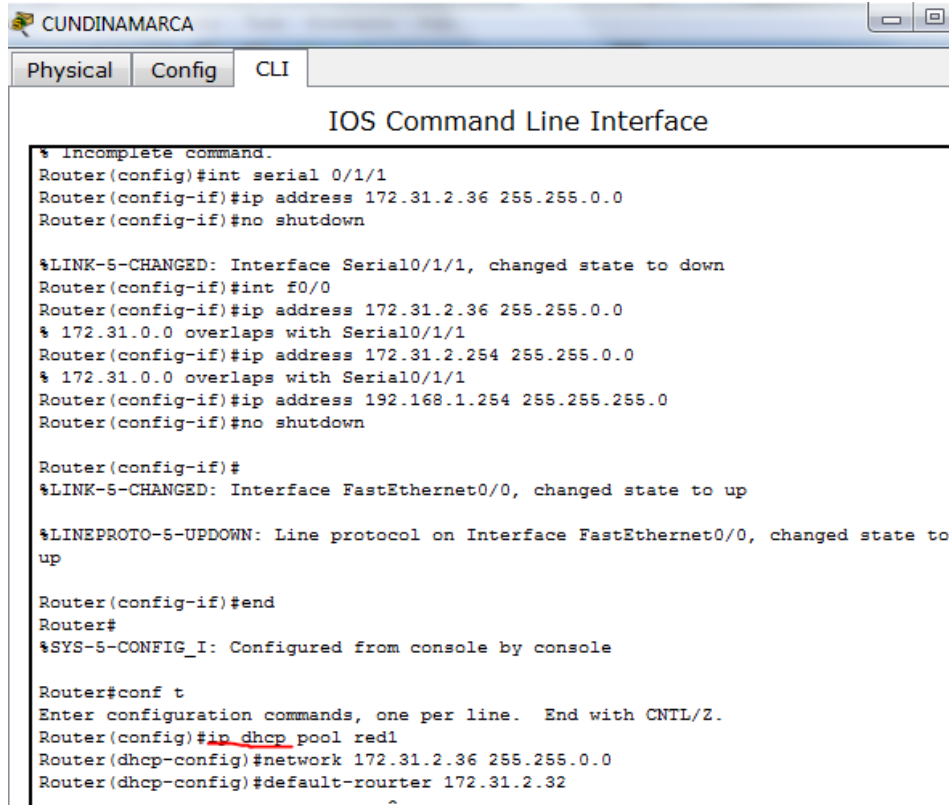


FIGURA 29 DHCP



```

* Incomplete command.
Router(config)#int serial 0/1/1
Router(config-if)#ip address 172.31.2.36 255.255.0.0
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/1, changed state to down
Router(config-if)#int f0/0
Router(config-if)#ip address 172.31.2.36 255.255.0.0
% 172.31.0.0 overlaps with Serial0/1/1
Router(config-if)#ip address 172.31.2.254 255.255.0.0
% 172.31.0.0 overlaps with Serial0/1/1
Router(config-if)#ip address 192.168.1.254 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to
up

Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp pool red1
Router(dhcp-config)#network 172.31.2.36 255.255.0.0
Router(dhcp-config)#default-router 172.31.2.32
  
```

FIGURA 30 DHCP CUNDINAMARCA

2.6 El web server deberá tener **NAT estático** y el resto de los equipos de la topología emplearán NAT de sobrecarga (PAT).

```

ip nat inside source static 1.1.1.1 2.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
permit ip any 30.1.10.128 0.0.0.127'
route-map R1 permit 10
match ip address ACL-A
  
```

Aspectos a tener en cuenta

- Habilitar VLAN en cada switch y permitir su enrutamiento.
- Enrutamiento OSPF con autenticación en cada router.

Bucaramanga

```

interface Loopback0
ip address 70.70.70.70 255.255.255.255
!
interface Serial0
  
```



PRUEBA DE HABILIDADES PRACTICAS CCNA

```
ip address 192.16.64.2 255.255.255.0
ip ospf message-digest-key 1 md5 c1$c0
```

!--- Message digest key with ID "1" and !--- Key value (password) is set as "c1\$c0 ".

```
clockrate 64000
!
router ospf 10
 network 192.16.64.0 0.0.0.255 area 0
 network 70.0.0.0 0.255.255.255 area 0
 area 0 authentication message-digest -->
```

!--- MD5 authentication is enabled for !--- all interfaces in Area 0.

Tunja

```
interface Loopback0
 ip address 172.16.10.36 255.255.255.240
!
interface Serial0
 ip address 192.16.64.1 255.255.255.0
 ip ospf message-digest-key 1 md5 c1$c0
```

!--- Message digest key with ID "1" and !--- Key (password) value is set as "c1\$c0 ".

```
!
router ospf 10
 network 172.16.0.0 0.0.255.255 area 0
 network 192.16.64.0 0.0.0.255 area 0
 area 0 authentication message-digest
```

!--- MD5 authentication is enabled for !--- all interfaces in Area 0.

Cundinamarca

show ip ospf interface serial0

```
Serial0 is up, line protocol is up
Internet Address 192.16.64.1/24, Area 0
Process ID 10, Router ID 172.16.10.36, Network Type POINT_TO_POINT,
. Cost: 64
Transmit Delay is 1 sec, State POINT_TO_POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:04
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 4 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
Simple password authentication enabled
```



2.7 Servicio DHCP en el router Tunja, mediante el helper address, para los routers Bucaramanga y Cundinamarca.

Accedemos privilegiado, luego configuración terminal

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

Colocamos un nombre al router en este caso Bucaramanga

```
Router(config)#hostname Bucaramanga
```

• Creamos el rango de ip quitadas del conjunto pool de direcciones que podrá asignar el servicio indicando la ip inicial y final del rango.

```
Bucaramanga (config)#ip dhcp excluded-addres 172.31.2.32 172.31.2.36
```

• **Ponemos un nombre al rango del servidor DHCP**

```
Bucaramanga(config)#ip dhcp pool DHCP_LAN_VENTAS
```

Definimos la red a la que dara servicio de DHCP

```
Bucaramanga(dhcp-config)#network 172.31.2.33 255.255.255.0
```

Puerta de enlace que ofrece al DHCP

```
Bucaramanga (dhcp-config)#default-router 172.31.2.34
```

Para terminar el DNS que entregará al DHCP

```
Bucaramanga(dhcp-config)#dns-server 8.8.8.8
```

Se debe tener en cuenta copiar la configuración del router que en este momento estan ejecutándose, en la configuración de inicio del router, en caso de que haya un bajón de energía o reinicio perderíamos la mayoría de información esto se hace con el siguiente comando:

```
Bucaramanga>enable
Bucaramanga#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

2.8 Configuración de NAT estático y de sobrecarga.

```
Tunja# show ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 209.165.200.226:51839 192.168.10.10:51839 209.165.201.1:80
209.165.201.1:80
tcp 209.165.200.226:42558 192.168.11.10:42558 209.165.202.129:80
209.165.202.129:80
Tunja#
```

Utilizamos el comando nat statistics comprueba las nat que haya asignado una dirección para ambas traducciones

```
Tunja# clear ip nat statistics
Tunja# show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 2 extended)
Peak translations: 2, occurred 00:00:05 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
Hits: 4 Misses: 0
CEF Translated packets: 4, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 3] access-list 1 pool NAT-POOL2 refcount 2
pool NAT-POOL2: netmask 255.255.255.224
  start 209.165.200.226 end 209.165.200.240
  type generic, total addresses 15, allocated 1 (6%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
Tunja#
```

Listas de control de acceso:

2.9 Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.

```
CUNDINAMARCA(config)#access-list 1 deny 172.31.2.8
255.255.255.0
CUNDINAMARCA(config)#access-list 1 permit 192.168.1.257

CUNDINAMARCA(config)#acc
CUNDINAMARCA(config)#interface fas
CUNDINAMARCA(config)#interfase fastethernet 1/0
```



```
CUNDINAMARCA(config)#acce
CUNDINAMARCA(config)#ip access-group out
CUNDINAMARCA(config)#
```

2.10 Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja

```
CUNDINAMARCA(config)#access-list 1 permit 192.168.1.257
255.255.255.0
CUNDINAMARCA(config)#access-list 1 permit 209.17.220.0
CUNDINAMARCA(config)#acc
CUNDINAMARCA(config)#interface fas
CUNDINAMARCA(config)#interfase fastethernet 0/0

CUNDINAMARCA(config)#acce
CUNDINAMARCA(config)#ip access-group out
CUNDINAMARCA(config)#.
```

3 Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.

```
TUNJA(config)#access-list 1 permit 172.31.0.192
255.255.255.0
TUNJA(config)#access-list 1 permit 209.17.220.0
TUNJA(config)#acc
TUNJA(config)#interface fas
TUNJA(config)#interfase fastethernet 1/0
TUNJA(config)#acce
TUNJA(config)#ip access-group out
TUNJA(config)#.
```

4 Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga

```
TUNJA(config)#access-list 1 permit 172.31.0.128
255.255.255.0
TUNJA(config)#access-list 1 permit 172.31.1.64
TUNJA(config)#acc
TUNJA(config)#interface fas
TUNJA(config)#interfase fastethernet 0/0
```

```
TUNJA(config)#acce
TUNJA(config)#ip access-group out
TUNJA(config)#.
TUNJA(config)#access-list 1 permit 172.31.2.8
TUNJA(config)#acc
TUNJA(config)#interface fas
TUNJA(config)#interfase fastethernet 0/1
TUNJA(config)#acce
TUNJA(config)#ip access-group out
TUNJA(config)#.
```

- 5 Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.

```
BUCARAMANGA(config)#access-list 1 permit 209.17.220.0
255.255.255.0
BUCARAMANGA (config)#access-list 1 permit any
172.31.0.0
BUCARAMANGA (config)#acc
BUCARAMANGA (config)#interface fas
BUCARAMANGA (config)#interfase fastethernet 0/2
BUCARAMANGA (config)#acce
BUCARAMANGA (config)#ip access-group out
BUCARAMANGA (config)#.
```

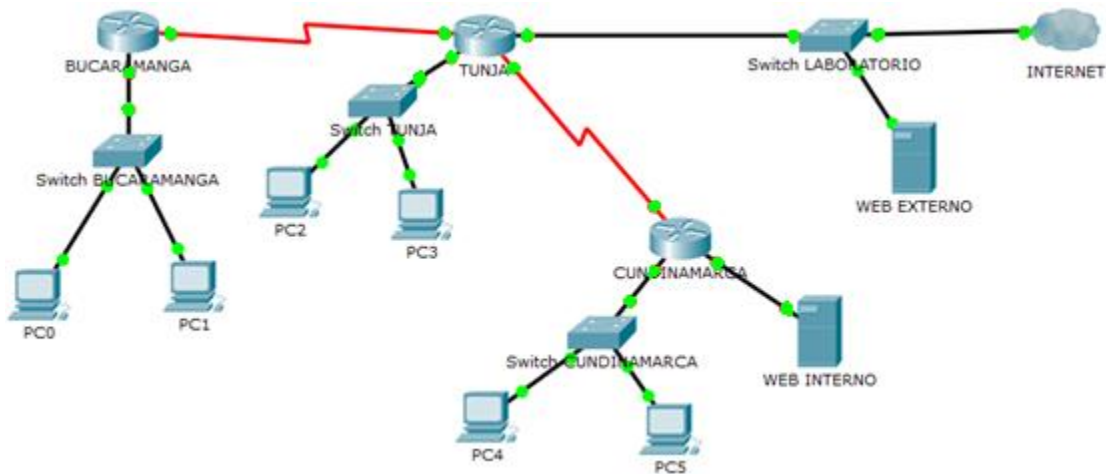
- 6 Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.

```
BUCARAMANGA(config)#access-list 1 permit 172.31.1.64
255.255.255.0
BUCARAMANGA (config)#access-list 1 permit any
172.31.0.0
BUCARAMANGA (config)#acc
BUCARAMANGA (config)#interface fas
BUCARAMANGA (config)#interfase fastethernet 0/2
BUCARAMANGA (config)#acce
BUCARAMANGA (config)#ip access-group out
BUCARAMANGA (config)#.
```

```

BUCARAMANGA (config)#access-list 1 deny 209.17.220.0
255.255.255.0
BUCARAMANGA (config)#access-list 1 permit any
172.31.0.192
BUCARAMANGA (config)#acc
BUCARAMANGA (config)#interface fas
BUCARAMANGA (config)#interface fastethernet 0/2
BUCARAMANGA (config)#acce
BUCARAMANGA (config)#ip access-group out
BUCARAMANGA (config)#.
  
```

2.11 PRUEBA DE CONECTIVIDAD:





CONCLUSIONES

El programa packet tracer permite el diseño y la configuración de los para la solución de los escenarios propuestos.

La exigencia académica del Diplomado Cisco, permitió el avance académico para el manejo de las situaciones planteadas en la problemática a abordar.

Los objetivos se cumplieron en su totalidad durante el desarrollo de la prueba de habilidades.

Existen protocolos fáciles y complejos con los cuales se puede direccionar una IP

El protocolo ayuda a que la red sea más segura y confiable, por medio de

La configuración que se necesite para salvaguardar los datos.

El protocolo EIGRP es sencillo y ayuda a saber los daños, a conocer los dispositivos vecinos, y ordenar las direcciones de las interfaces

BIBLIOGRAFIA

CICO NETWORKING ACADEMY – CCNA 1

<https://static-course-assets.s3.amazonaws.com/ITN503/es/index.html>

UNAD (2014). Ping y Tracer como estrategias en procesos de Networking [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1lhgTCtKY-7F5KIRC3>

UNAD (2014). Ping y Tracer como estrategias en procesos de Networking [OVA]. Recuperado de <https://1drv.ms/u/s!AmIJYei-NT1lhgTCtKY-7F5KIRC3>

Cisco CCNA – configuración DHCP <http://blog.capacityacademy.com/2014/01/09/cisco-ccna-como-configurar-dhcp-en-cisco-router/>

CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1>

Como configurar OPSF en Router <http://blog.capacityacademy.com/2014/06/23/cisco-ccna-como-configurar-ospf-en-cisco-router/>

CISCO. (2014). Soluciones de Red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1>

Configuración troncal 802.1Q

https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-4000-series-switches/24064-171.html